WHAT IS CLAIMED IS:

1. An image processing system comprising:

an image providing apparatus which provides an image file, from which a digital watermark information can be extracted by using a watermark key that includes an authentication information which authenticates said image file provided by an valid provider, and said watermark key of said image file; and

an image utilizing apparatus which extracts said digital watermark information from said image file provided by said image providing apparatus using said watermark key provided by said image providing apparatus, verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key, and displays said verified image file.

2. An image processing system comprising:

an image providing apparatus which provides an image file, from which a digital watermark information can be extracted using a watermark key that includes an authentication information which authenticates said image file provided by an valid provider; and

an image utilizing apparatus which generates a watermark key which includes an authentication information that authenticates said image file provided by said valid provider, extracts said digital watermark information from said image file provided by said image providing apparatus using said generated watermark key, verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key, and displays said verified image file.

3. An image processing system comprising:

an image providing apparatus which generates a watermark key which includes an authentication information that authenticates an image file provided by a valid provider, embeds a digital watermark, which can be extracted by using said watermark key, in said image file, and provides said image file and said watermark key;

an image managing apparatus which extracts said digital watermark information from said image file provided by said image providing apparatus using said watermark key provided by said image providing apparatus, verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key, stores said verified image file and said verified watermark key, and provides said verified image file and said verified watermark key to a user; and

an image utilizing apparatus which extracts said digital watermark information from said image file provided by said image managing apparatus using said watermark key provided by said image managing apparatus, verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key, and displays said verified image file.

4. An image processing system comprising:

an image providing apparatus which generates a watermark key which includes an authentication information that authenticates an image file provided by a valid provider, embeds a digital watermark, which can be extracted, in said image file by said watermark key, and provides said image file;

an image managing apparatus which generates a watermark key which includes an authentication information that authenticates said image file provided by said valid provider, extracts said

digital watermark information from said image file provided by said image providing apparatus using said watermark key, verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key, stores said verified image file, and provides said verified image file to a user; and

an image utilizing apparatus which generates a watermark key which includes an authentication information that authenticates said image file provided by said valid provider, extracts said digital watermark information from said image file provided by said image managing apparatus using said watermark key, verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key, and displays said verified image file.

5. An image processing system comprising:

an image providing apparatus which generates a watermark key which includes an authentication information that authenticates an image file provided by a valid provider, embeds a digital watermark, which can be extracted, in said image file by said watermark key, and provides said image file;

an image managing apparatus which generates a watermark key which includes an authentication information that authenticates said image file provided by said valid provider, extracts said digital watermark information from said image file provided by said image providing apparatus using said watermark key, verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key, stores said verified image file, associates an additional information, which includes an

authentication information that authenticates said image file provided by said valid provider, with said image file, and provides said image file with said additional information to a user; and

an image utilizing apparatus which extracts said authentication information from said additional information, generates a watermark key which includes said authentication information, extracts said digital watermark information from said image file provided by said image managing apparatus using said watermark key, verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, verifies whether said image file has been tampered or not using said verified watermark key, and displays said verified image file.

6. An image processing system as claimed in claim 1, wherein said image utilizing apparatus generates said authentication information which authenticates said image file provided by said valid provider, and compares said generated authentication information with an authentication information extracted from said provided watermark key to verify whether said provided watermark key is valid.

7. An image processing system as claimed in claim 3, wherein said image managing apparatus generates said authentication information which authenticates said image file provided by said valid provider, and compares said generated authentication information with an authentication information extracted from said provided watermark key to verify whether said provided watermark key is valid.

8. An image processing system as claimed in claim 3, wherein said image utilizing apparatus generates said authentication information which authenticates said image file provided by said

valid provider, and compares said generated authentication information with an authentication information extracted from said provided watermark key to verify whether said provided watermark key is valid.

9. An image processing system as claimed in claim 3, wherein:

said image managing apparatus associates an additional information, which includes an authentication information that authenticates said image file provided by said valid provider, with said image file, provides said image file with said additional information to a user; and

said image utilizing apparatus extracts said authentication information in said additional information, generates a watermark key which includes said authentication information, extracts said information of said digital watermark from said image file provided by said image managing apparatus by said watermark key, verifies whether said image file has been tampered or not, and displays said verified image file.

10. An image processing system as claimed in any of claim 1 to 5, wherein said authentication information includes a provider identifying information which identifies said provider of said image file or an image identifying information which identifies said image file.

11. An image utilizing apparatus comprising:

an inputting means which inputs a watermark key and an image file;

an extracting means which extracts a digital watermark information from said image file using said watermark key;

a watermark key verifying means which verifies whether said watermark key has been tampered or not using an authentication information, which authenticates said image file provided by a valid provider, in said watermark key;

an image file verifying means which verifies whether said image file has been tampered or not using said verified watermark key; and

a displaying means which displays said verified image file.

12. An image utilizing apparatus comprising:

an inputting means which inputs an image file;

a generating means which generates a watermark key which includes an authentication information which authenticates said image file provided by a valid provider;

an extracting means which extracts said digital watermark information from said image file using said watermark key;

a watermark key verifying means which verifies whether said input watermark key has been tampered or not using said authentication information in said watermark key;

an image file verifying means which verifies whether said image file has been tampered or not using said verified watermark key; and

a displaying means which displays said verified image file.

13. An image utilizing apparatus comprising:

an inputting means which inputs an additional information, which includes an authentication information which authenticates said image file provided by a valid provider, with an image file;

an extracting means which extracts said authentication information from said additional information;

a generating means which generates a watermark key which includes said authentication information;

an extracting means which extracts said digital watermark information from said image file using said watermark key;

a watermark key verifying means which verifies whether said watermark key has been tampered or not using said authentication information in said watermark key;

an image file verifying means which verifies whether said

image file has been tampered or not using said verified watermark key; and

a displaying means which displays said verified image file.

14. An image utilizing apparatus as claimed in claim 11, further comprising a generating means which generates said authentication information which authenticates said image file provided by said valid provider; and wherein said watermark key verifying means which compares said generated authentication information with an authentication information extracted from said input watermark key to verify whether said input watermark key is valid.

15. An image utilizing apparatus as claimed in any of claim 11 to 13, wherein said authentication information includes a provider identifying information which identifies said provider of said image file or an image identifying information which identifies said image file.

16. An image managing apparatus comprising:

an inputting means which inputs a watermark key and an image file;

an extracting means which extracts said digital watermark information from said image file using said watermark key;

a watermark key verifying means which verifies whether said watermark key has been tampered or not using an authentication information, which authenticates said image file provided by a valid provider, in said watermark key, and

an image file verifying means which verifies whether said image file has been tampered or not using said verified watermark key;

a storing means which stores said verified image file and said verified watermark key; and

a providing means which provides said verified image file and said verified watermark key to a user.

17. An image managing apparatus comprising:

an inputting means which inputs an image file;

a generating means which generates a watermark key which includes an authentication information which authenticates said image file provided by a valid provider;

an extracting means which extracts said digital watermark information from said image file using said watermark key;

a watermark key verifying means which verifies whether said watermark key has been tampered or not using said authentication information in said watermark key;

an image file verifying means which verifies whether said image file has been tampered or not using said verified watermark key;

a storing means which stores said verified image file; and

a providing means which provides said verified image file to a user.

18. An image managing apparatus comprising:

an inputting means which inputs an image file;

a generating means which generates a watermark key which includes an authentication information which authenticates said image file provided by a valid provider;

an extracting means which extracts said digital watermark information from said image file using said watermark key;

a watermark key verifying means which verifies whether said watermark key has been tampered or not using said authentication information in said watermark key;

an image file verifying means which verifies whether said image file has been tampered or not using said verified watermark key;

a storing means which stores said verified image file; and

a providing means which adds an additional information which includes said authentication information to said image file,

and provides said image file with said additional information to a user.

19. An image managing apparatus as claimed in claim 16, further comprising a generating means which generates said authentication information which authenticates said image file provided by said valid provider; and wherein said watermark key verifying means which compares said generated authentication information with an authentication information extracted from said input watermark key to verify whether said input watermark key is valid.

20. An image managing apparatus as claimed in any of claim 16 to 18, wherein said authentication information includes a provider identifying information which identifies said provider of said image file or an image identifying information which identifies said image file.

21. A recording medium storing a program to be executed by a computer, said program comprising:

an inputting module which inputs a watermark key and an image file;

an extracting module which extracts a digital watermark information from said image file using said watermark key;

a watermark key verifying module which verifies whether said watermark key has been tampered or not using an authentication information, which authenticates said image file provided by a valid provider, in said watermark key;

an image file verifying module which verifies whether said image file has been tampered or not using said verified watermark key; and

a displaying module which displays said verified image file.

22. A recording medium storing a program to be executed by a

computer, said program comprising:

an inputting module which inputs an image file;

a generating module which generates a watermark key which includes an authentication information which authenticates said image file provided by a valid provider;

an extracting module which extracts said digital watermark information from said image file using said watermark key;

a watermark key verifying module which verifies whether said input watermark key has been tampered or not using said authentication information in said watermark key;

an image file verifying module which verifies whether said image file has been tampered or not using said verified watermark key; and

a displaying module which displays said verified image file.

23. A recording medium storing a program to be executed by a computer, said program comprising:

an inputting module which inputs an additional information, which includes an authentication information which authenticates said image file provided by a valid provider, with an image file;

an extracting module which extracts said authentication information from said additional information;

a generating module which generates a watermark key which includes said authentication information, and

an extracting module which extracts said digital watermark information from said image file using said watermark key;

a watermark key verifying module which verifies whether said watermark key has been tampered or not using said authentication information in said watermark key;

an image file verifying module which verifies whether said image file has been tampered or not using said verified watermark key; and

a displaying module which displays said verified image

file.

24. A recording medium storing a program to be executed by a computer, said program comprising:

an inputting module which inputs a watermark key and an image file;

an extracting module which extracts said digital watermark information from said image file using said watermark key;

a watermark key verifying module which verifies whether said watermark key has been tampered or not using an authentication information, which authenticates said image file provided by a valid provider, in said watermark key, and

an image file verifying module which verifies whether said image file has been tampered or not using said verified watermark key;

a storing module which stores said verified image file and said verified watermark key; and

a providing module which provides said verified image file and said verified watermark key to a user.

25. A recording medium storing a program to be executed by a computer, said program comprising:

an inputting module which inputs an image file;

a generating module which generates a watermark key which includes an authentication information which authenticates said image file provided by a valid provider;

an extracting module which extracts said digital watermark information from said image file using said watermark key;

a watermark key verifying module which verifies whether said watermark key has been tampered or not using said authentication information in said watermark key, and

an image file verifying module which verifies whether said image file has been tampered or not using said verified watermark key;

a storing module which stores said verified image file; and

a providing module which provides said verified image file to a user.

26. A recording medium storing a program to be executed by a computer, said program comprising:

an inputting module which inputs an image file;

a generating module which generates a watermark key which includes an authentication information which authenticates said image file provided by a valid provider, and

an extracting module which extracts said digital watermark information from said image file using said watermark key;

a watermark key verifying module which verifies whether said watermark key has been tampered or not using said authentication information in said watermark key;

an image file verifying module which verifies whether said image file has been tampered or not using said verified watermark key;

a storing module which stores said verified image file;

a providing module which adds an additional information which includes said authentication information to said image file, and provides said image file with said additional information to a user.

27. An image verifying method comprising:

inputting a watermark key and an image file;

extracting a digital watermark information from said image file using said watermark key;

verifying whether said watermark key has been tampered or not using an authentication information, which authenticates said image file provided by a valid provider, in said watermark key; and

verifying whether said image file has been tampered or not using said verified watermark key.

28. An image verifying method comprising:

inputting an image file;

generating a watermark key which includes an authentication information which authenticates said image file provided by a valid provider;

extracting said digital watermark information from said image file using said watermark key;

verifying whether said input watermark key has been tampered or not using said authentication information in said watermark key; and

verifying whether said image file has been tampered or not using said verified watermark key.

29. An image verifying method comprising:

inputting an additional information, which includes an authentication information which authenticates said image file provided by a valid provider, with an image file;

extracting said authentication information from said additional information;

generating a watermark key which includes said authentication information;

extracting said digital watermark information from said image file using said watermark key;

verifying whether said watermark key has been tampered or not using said authentication information in said watermark key; and

verifying whether said image file has been tampered or not using said verified watermark key.

30. An image verifying method as claimed in claim 27, further comprising generating said authentication information which authenticates said image file provided by said valid provider; and wherein said verifying said watermark key compares said

generated authentication information with an authentication information extracted from said input watermark key to verify whether said input watermark key is valid.

31. An image verifying method as claimed in any of claim 27 to 29, wherein said authentication information includes a provider identifying information which identifies said provider of said image file or an image identifying information which identifies said image file.

32. An image processing system as claimed in claim 1 or 2, wherein:

said image providing apparatus defines a location information for embedding said digital watermark in a part of a region in said image file, and provides said image file in which said digital watermark is embedded based on said location information; and

said image utilizing apparatus extracts said digital watermark from said image file provided by said image providing apparatus based on said location information, and verifies whether a data in said part of a region, in which said digital watermark is embedded, has been tampered.

33. An image processing system as claimed in claim 1 or 2, wherein:

said image providing apparatus recognizes a format of said image file, and provides said image file in which said digital watermark is embedded in a part of a region based on said format; and

said image utilizing apparatus recognizes said format of said image file provided by said image providing apparatus, extracts said digital watermark from said part of a region based on said format, and verifies whether a data in said part of a region, in which said digital watermark is embedded, has been tampered.

34. An image processing system comprising:

an image providing apparatus which defines a location information for embedding a digital watermark in a part of a region in an image file and provides said image file, in which said digital watermark is embedded based on said location information; and

an image utilizing apparatus which extracts said digital watermark from said image file provided by said image providing apparatus based on said location information, and verifies whether a data in said part of a region, in which said digital watermark is embedded, has been tampered.

35. An image processing system comprising:

an image providing apparatus which recognizes a format of an image file and provides said image file in which a digital watermark is embedded in a part of a region based on said format; and

an image utilizing apparatus which recognizes said format of said image file, extracts said digital watermark from said part of a region based on said format, and verifies whether a data in said part of a region in said image file, in which said digital watermark is embedded, has been tampered.

36. An image processing system as claimed in claim 34 or 35, wherein said image providing apparatus provides said image file in which a different kind of said digital watermark is embedded in a different region in said image file.

37. An image processing system as claimed in claim 36, wherein said image providing apparatus provides said image file in which a different kind of said digital watermark is embedded according to an image quality in each region where said digital watermark is embedded.

38. An image processing system as claimed in claim 34, wherein:

said location information for embedding a digital watermark includes a location information of a region for displaying a specific information necessary for detecting a tamper; and

said image utilizing apparatus extracts said digital watermark with said message digest from said image file based on said location information, and generates a corresponding message digest using said specific information in said provided image file, and detects tampering with said image file by comparing said extracted message digest with said corresponding generated message digest.

39. An image processing system as claimed in claim 34, wherein:

said location information for embedding a digital watermark includes a location information of a region for displaying a specific information necessary for detecting a tamper and a location information of a region for embedding a message digest corresponding to said specific information; and

said image utilizing apparatus extracts said digital watermark with said message digest from said image file based on said location information, generates a corresponding message digest using said specific information in said provided image file, and detects tampering with said image file by comparing said extracted message digest with said corresponding generated message digest.

40. An image processing system as claimed in claim 39, wherein said region for embedding said message digest corresponding to said specific information is independent of said region for displaying said specific information necessary for detecting said tamper.

41. An image processing system as claimed in claim 34, wherein:

said location information is registered in both of said

image providing apparatus and said image utilizing apparatus;

said image providing apparatus embeds said digital watermark in said image file based on said registered location information; and

said image utilizing apparatus extracts said digital watermark from said image file based on said registered location information.

42. An image processing system as claimed in claim 34, wherein:

said image providing apparatus transfers said location information to said image utilizing apparatus;

said image providing apparatus embeds said digital watermark in said image file based on said location information to be transferred; and

said image utilizing apparatus extracts said digital watermark from said image file based on said location information transferred from said image providing apparatus.

43. An image providing apparatus comprising:

a location defining means which defines a location information for embedding a digital watermark in a part of a region in an image file; and

a providing means which provides said image file in which said digital watermark is embedded based on said location information.

44. An image providing apparatus comprising:

a format recognizing means which recognizes a format of an image file; and

a providing means which provides said image file in which a digital watermark is embedded in a part of a region based on said format.

45. An image providing apparatus as claimed in claim 43 or 44,

wherein said providing means provides said image file in which a different kind of said digital watermark is embedded in a different region in said image file.

46. An image providing apparatus as claimed in claim 45, wherein said providing means provides said image file in which a different kind of said digital watermark is embedded according to an image quality in each region where said digital watermark is embedded.

47. An image providing apparatus as claimed in claim 43, wherein said location information for embedding a digital watermark includes a location information of a region for displaying a specific information necessary for detecting a tamper and a location information of a region for embedding a message digest corresponding to said specific information.

48. An image providing apparatus as claimed in claim 47, wherein said region for embedding said message digest corresponding to said specific information is independent of said region for displaying said specific information necessary for detecting said tamper.

49. An image utilizing apparatus comprising:

an inputting means which inputs an image file in which a location information is defined for embedding a digital watermark in a part of a region in said image file;

an extracting means which extracts said digital watermark from said image file based on said location information; and

a verifying means which verifies whether a data in said part of a region, in which said digital watermark is embedded, has been tampered.

50. An image utilizing apparatus comprising:

an inputting means which inputs an image file;

a format recognizing means which recognizes said format of said image file;

an extracting means which extracts said digital watermark from said part of a region based on said format; and

a verifying means which verifies whether a data in said part of a region, in which said digital watermark is embedded, has been tampered.

51. An image utilizing apparatus as claimed in claim 49, further comprising a generating means which generates a corresponding message digest using said specific information in said input image file, and wherein:

said extracting means which extracts said digital watermark with said message digest from said image file based on said location information; and

said verifying means which detects tampering with said image file by comparing said extracted message digest with said corresponding generated message digest.

52. A recording medium storing a program to be executed by a computer, said program comprising:

a location defining module which defines a location information for embedding a digital watermark in a part of a region in an image file; and

a providing module which provides said image file in which said digital watermark is embedded based on said location information.

53. A recording medium storing a program to be executed by a computer, said program comprising:

a format recognizing module which recognizes a format of an image file; and

a providing module which provides said image file in which a digital watermark is embedded in a part of a region based on

said format.

54. A recording medium as claimed in claim 52 or 53, wherein said providing module provides said image file in which a different kind of said digital watermark is embedded in a different region in said image file.

55. A recording medium as claimed in claim 54, wherein said providing module provides said image file in which a different kind of said digital watermark is embedded according to an image quality in each region where said digital watermark is embedded.

56. A recording medium as claimed in claim 52, wherein said location information for embedding a digital watermark includes a location information of a region for displaying a specific information necessary for detecting a tamper and a location information of a region for embedding a message digest corresponding to said specific information.

57. A recording medium as claimed in claim 56, wherein said region for embedding said message digest corresponding to said specific information is independent of said region for displaying said specific information necessary for detecting said tamper.

58. A recording medium storing a program to be executed by a computer, said program comprising:

an inputting module which inputs an image file in which a location information is defined for embedding a digital watermark in a part of a region in said image file;

an extracting module which extracts said digital watermark from said image file based on said location information; and

a verifying module which verifies whether a data in said part of a region, in which said digital watermark is embedded, has been tampered.

59. A recording medium storing a program to be executed by a computer, said program comprising:

an inputting module which inputs an image file;

a format recognizing module which recognizes said format of said image file;

an extracting module which extracts said digital watermark from said part of a region based on said format; and

a verifying module which verifies whether a data in said part of a region, in which said digital watermark is embedded, has been tampered.

60. A recording medium as claimed in claim 58, further comprising a generating module which generates a corresponding message digest using said specific information in said input image file, and wherein:

said extracting module which extracts said digital watermark with said message digest from said image file based on said location information; and

said verifying module which detects tampering with said image file by comparing said extracted message digest with said corresponding generated message digest.

61. An image verifying method comprising:

inputting an image file in which a location information is defined for embedding a digital watermark in a part of a region in said image file;

extracting said digital watermark from said image file based on said location information; and

verifying whether a data in said part of a region, in which said digital watermark is embedded, has been tampered.

62. An image verifying method comprising:

inputting an image file;

recognizing said format of said image file;

extracting said digital watermark from said part of a region based on said format; and

verifying whether a data in said part of a region, in which said digital watermark is embedded, has been tampered.

63. An image verifying method as claimed in claim 61, further comprising generating a corresponding message digest using said specific information in said input image file, and wherein:

said extracting said digital watermark extracts said digital watermark with said message digest from said image file based on said location information; and

said verifying tampering detects tampering with said image file by comparing said extracted message digest with said corresponding generated message digest.